International Journal of Electrical and Electronics Engineering Research (IJEEER)
ISSN(P): 2250-155X; ISSN(E): 2278-943X
Vol. 4, Issue 2, Apr 2014, 33-40

TRANS STELLAR
▪ Journal Publications ▪ Research Consultancy

OPTIMUM OPERATIONAL COST ALGORITHM FOR CRYPTOGRAPHY OF MULTIMEDIA DATA

ATUL S. JOSHI[1] & P. R. DESHMUKH[2]

[1]Department of Electronics & Telecommunication Engineering, Dr.Panjabrao Deshmukh College of Engineering, Amravati, Maharashtra, India

[2]Department of, Computer Science & Engineering, Dr.Panjabrao Deshmukh College of Engineering, Amravati, Maharashtra, India

ABSTRACT

From the last decade the world is experiencing the unprecedented explosion in the amount of multimedia data. Hence security of this data is an important issue. The aspects of information security can address by cryptography. Cryptography is the practice of storing and communicating data in such a form that only whom it is intended for can read and process. In this paper we propose optimum operational cost encoding technique which offers higher compression ratios and better security towards the cryptanalysis attacks during transmission of the multimedia data. It is simple, low complexity algorithm and suitable for text, image as well as audio applications. At the transmitter side, source file is first converted into binary form. Source bit stream is decompose to the blocks of equal length, (X_i). Pseudorandom generator is used to generate secured key, (Y_i). From the pair of bits in the block, a sequence number is calculated i.e. $\sum_{i=0}^{1} \boldsymbol{Xi} * 2^i$. This number selects the particular bits in the key bit of the key. This bit is then complemented. For each chunk, the pseudorandom generator generates a new key which provide integrity protection, in addition to confidentiality. A selective encryption technique is employed in this algorithm. Hamming Distance in between the Y_i & ΔY_i are taken care by the algorithm thereafter to form a codebook. At the receiver side, cipher extracted from the channel is decompressed and decrypt jointly with the help of codebook and secret key. Decompression and Decryption of the compressed cipher is again integrated process in this algorithm. Entire bit stream is then obtained from the chunk of bits which thereafter converted to original source data. Due joint execution of encryption and compression processes this algorithm provides high degree of security with better compression performance at very low operational cost.

KEYWORDS: Hamming Distance, Polygram Substitution, Key, Encryption and Compression